Association for Information Systems
AIS Electronic Library (AISeL)

MWAIS 2018 Proceedings | Midwest (MWAIS)

5-2018

Fear and Loathing of Cybersecurity: What Keeps IT Executives Awake at Night

Steven A. Wallace
University of Toledo, steve.wallace@utoledo.edu

Karen Y. Green
University of Toledo, karen.green@utoledo.edu

Fear and Loathing of Cybersecurity: What Keeps IT Executives Awake at Night

Steven A Wallace
University of Toledo
steve.wallace@utoledo.edu

Karen Y Green
University of Toledo
karen.green@utoledo.edu

ABSTRACT

Recent high-profile incidents have engendered doubts about trust in various firms and have resulted in cyber security becoming a critical risk factor that firms must address. Unsurprisingly, data breaches are currently the biggest concern of CIOs. The goal of this research is to answer the following questions: *What are the specific cyber security concerns of the organization's leaders, and how will those leaders allocate resources to allay those concerns?* We intend to use the Technology-Organization-Environment (TOE) Framework through a multiple case study approach. We will be collecting qualitative data through the use of semi-structured interviews of CIOs that are working in various industries in the US Midwest. The goal of this study is to extend the TOE framework to best explain the executive decision process with regards to cyber security.

Keywords (Required)

IT Leaders, Cybersecurity, TOE Framework, Qualitative Research, Executive Decision Making.

INTRODUCTION

Recent high-profile incidents, such as the 2014 Yahoo data breach compromising 1 billion accounts, and the 2017 Equifax breach compromising the social security numbers of 143 million Americans (Armerding, 2018) have engendered doubts about trust in these firms and have resulted in cyber security becoming a critical risk factor that firms must address. A cyber security breach is defined as malicious or benign unauthorized access of information. The data that may be stolen often contains sensitive information such as social security numbers, credit card numbers, private patient information, trade secrets, and other proprietary corporate information. Breaches can precipitate extreme consequences for managers, shareholders and customers of the affected firm. Cyber security breaches in aggregate across organizations have resulted in billions of dollars lost annually (Cerrudo, 2017). Specifically, the financial impact can be felt with lost sales, fines, and settlement costs (Deloitte, 2016). Additionally, there are the indirect costs associated with reputational damage and customer flight that may lead to longer-term losses of market share. Unsurprisingly, data breaches are currently the biggest concern of IT leaders (Kappelman et al., 2017).

The goal of this research is to answer the following questions: *What are the specific cyber security concerns of the organization's leaders, and how will those leaders allocate resources to allay those concerns?* In order to answer these questions, we will be using the multiple case study methodology. We will be collecting qualitative data through the use of semi-structured interviews of CIOs that are working in various industries in the US Midwest. In order to search for a richer understanding of this phenomenon, we will use an interpretive approach (Klein & Myers, 1999). An interpretive analysis will also give us a better understanding of the relationships between technostress and EMR usage and any other constructs that we discover in our research.

We will be using the Technology-Organization-Environment (TOE) Framework (DePietro et al., 1990). This framework has been used in prior IS adoption studies for Knowledge Management Systems (Lin, 2014), Enterprise-level 2.0 applications (Jia et al., 2017), and software-as-a-service (Yang et al., 2015). We will use this theory to help formulate our data collection and analysis.

TECHNOLOGY-ORGANIZATION-ENVIRONMENT FRAMEWORK

The Executive level analysis will be based on the Technology-Organization-Environment (TOE) framework (DePietro et al., 1990). This established framework is primarily an information systems (IS) theory that deals with how IS adoption decisions are made. The general idea is that external factors (environment), organizational characteristics, and existing technology interact with one another to influence adoption decision making. An overview of the TOE Framework can be found below

(Figure 1). This framework, will allow us to examine the research questions: (1) What are the specific cyber security concerns of the organization's leaders, and (2) How will those leaders allocate resources to allay those concerns?

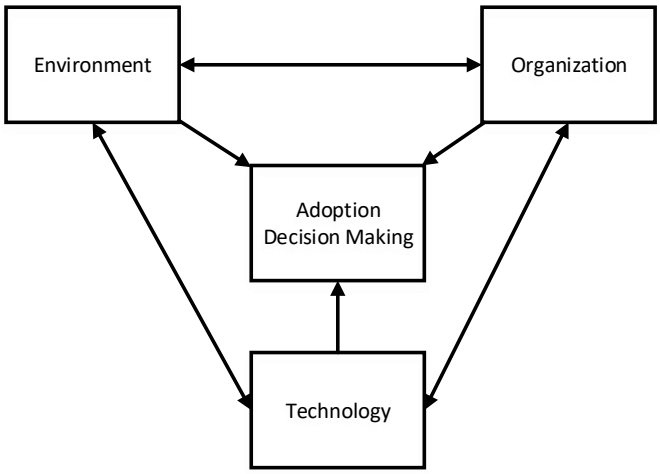

Figure 1: TOE Framework (DePietro et al., 1990)

Environment includes industry characteristics, government regulations (local, state, and federal), and the existing IT infrastructure. Environment also includes the firm's relationships with its partners and how that influences their technology and policy choices. In addition, how does the choices of their competitors impact their own decisions? Organizational characteristics include the IT processes and policies, organizational culture, size, and geographic location. Those characteristics also include the CIO behaviors and what resources are available for cybersecurity adoption. When observing existing technology, we include both the characteristics of that technology as well as its availability. When combined, those three factors influence the leader's decisions on whether to adopt those technologies.

Cyber security entails a two-pronged approach where policy is just as important as technology when protecting an organization's assets (Anderson & Agarwal, 2010). A highly secured IT infrastructure will not prevent a breach when a user unwittingly gives their authentication information away in a phishing attack. To reflect that reality, we will focus on the leader's decisions to both adopt existing technologies and any policy changes. An organization has a limited amount of resources, so our study will examine how executives allocate those resources (time, money, and labor) in protecting their organization's assets.

METHODOLOGY

To help answer our research question, we will use a multiple case study design outlined by Yin (2003). We will search for a richer understanding of the phenomenon under study through the use of an interpretive approach (Klein & Myers, 1999). Furthermore, we will use an established framework to help guide us in our interview question selection and data analysis (Walsham, 2006). Case studies are an excellent method for both testing and generating theory (Eisenhardt, 1989).

This portion of our project will focus on executives in manufacturing, non-profit, and service. We will use semi-structured interviews to collect our data from executives in positions who make major IS adoption decisions and who can help inform our study. With permission and IRB approval, these interviews will be audio recorded and transcribed. Those transcriptions will be analyzed by the entire research team and coded based on category (Miles & Huberman, 1994). Instead of trying to analyze pages of transcripts, this technique enables us to categorize chunks of the quotes into manageable pieces that can be compared and contrasted across subjects. Using initial codes based on our theoretical framework, the transcriptions will be analyzed using Atlas.ti. Once the coding is finished, the codes will be separated out and grouped. Those groups will help us understand any underlying constructs and how they interact with one another.

CONCLUSION

Specifically, we plan to extend the TOE framework to best explain the executive decision process with regards to cyber security. We will also have a list of specific cyber security issues and why they are important to the different leaders and organizations. In addition, we will identify their responses to these issues which can help build a new framework for this phenomenon. This in turn can spur explanatory research into the area of executive decision making with regards to

cybersecurity. This should provide a foundation for further explanatory research in terms of both quantitative and qualitative studies. For practical implications, this study can provide best practices for cyber security spending and policy.

REFERENCES

1. Anderson, C. L. and Agarwal, R. (2010) Practicing Safe Computing: A Multimedia Empirical Examination of Home Computer User Security Behavioral Intentions, *MIS quarterly*, 34, 3, 613-643.
2. Armerding, T. (2018, January 26) The 17 Biggest Data Breaches of the 21st Century, Retrieved from CSO: https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html
3. Cerrudo, C. (2017, January 17) Why Cybersecurity should be the biggest concern of 2017, Retrieved from Forbes: https://www.forbes.com/sites/forbestechcouncil/2017/01/17/why-cybersecurity-should-be-the-biggest-concern-of-2017/2/#7c6dd587274c
4. Deloitte. (2016) Lessons from the front line: Global cyber executive briefing, Retrieved from Deloitte.com: https://www2.deloitte.com/nz/en/pages/risk/articles/Global-Cyber-Briefing.html#
5. Depietro, R., Wiarda E., & Fleischer, M. (1990) The Context for Change: Organization, Technology and Environment, in Tornatzky, L.G. and Fleischer, M. (Eds.) *The Processes of Technological Innovation*, Lexington, MA: Lexington Books 151-175.
6. Eisenhardt, K. M. (1989). Building Theories from Case Study Research, *Academy of Management Review*, *14*, 4, 532–550.
7. Jia, Q., Guo, Y., and Barnes, S. J. (2017) Enterprise 2.0 post-adoption: Extending the information system continuance model based on the technology-Organization-environment framework, *Computers in Human Behavior*, *67*, 95-105.
8. Kappelman, L., Nguyen, Q., McLean, E., Maurer, C., Johnson, V., Snyder, M., and Torres, R. (2017) The 2016 SIM IT Issues and Trends Study. *MIS Quarterly Executive*, *16*, 1.
9. Klein, H. K., and Myers, M. D. (1999) A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems, *MIS Quarterly*, *23*, 1, 67.
10. Lin, H. F. (2014) Contextual factors affecting knowledge management diffusion in SMEs. *Industrial Management & Data Systems*, *114*, 9, 1415-1437.
11. Miles, M. B., and Huberman, A. M. (1994) *Qualitative data analysis: A sourcebook.* Beverly Hills: Sage Publications.
12. Walsham, G. (2006) Doing Interpretive Research, *European Journal of Information Systems*, *15*, 3, 320–330.
13. Yang, Z., Sun, J., Zhang, Y., and Wang, Y. (2015) Understanding SaaS adoption from the perspective of organizational users: A tripod readiness model, *Computers in Human Behavior*, *45*, 254-264.
14. Yin, R. K. (2003) *Case Study Research: Design and Methods* (4th ed., Vol. 5). Thousand Oaks, CA: SAGE.